APPENDIX A

In the Specification:

Page 1, line 2, insert the following paragraph:

Priority of application no. 2000-15161 filed on 29 May, 2000 in Republic of Korea and priority of application no. 2000-32182 filed on 06 December, 2000 in Republic of Korea are claimed under 35 U.S.C. § 119.

The paragraph at page 2, line 6, is revised as follows:

On the other hand, the corporate branches can enjoy the security of the private computer network via access control and encryption, while taking advantage of the economies of scale and built-in management facilities of large public networks. For example, the point-to-point tunneling protocol (PPTP) that encapsulates other protocol for transmission over an IP (Internet Protocol) network is used to create a VPN (Virtual Private Network) within the public Internet. The VPN allows a network manager to connect corporate remote branch sites and/or project teams to the corporate main branch economically and provides remote access to employees, which reduces the in-house requirements for equipment and support. That is, an Internet-based VPN uses the open, distributed infrastructure of the Internet to transmit data between corporate branches.

The paragraph at page 2, line 21, is revised as follows:

Since each of the corporate branches is connected to the Internet in the Internet-based VPN, information can be exchanged between the VPN users and the Internet users. This information exchange presents a challenge to protect information located on the corporate branches from unauthorized access by the Internet users and from unauthorized export by the VPN users. For example, [crackers] hackers have been able to erase files or disks, cancel programs, retrieve sensitive information and even introduce computer viruses, Trojan horses and/or worms into the corporate main branch.

The paragraph at page 3, line 6, is revised as follows:

A firewall is a technique for keeping a network secure. The firewall is widely used to separate corporate public resources, e.g., DMZ (Demilitarized Zone) servers including a corporate

public Web server, mail server, [and etc,] etc., from a corporate internal network as well as to give the VPN users access to the Internet in a secure fashion.

The paragraph at page 5, line 14, is revised as follows:

In accordance with one aspect of the present invention, there is provided an integrated security gateway apparatus interfacing with an internal network and an external network for blocking a selected packet from the internal network or external network, comprising a packet duplicating module for receiving and duplicating an incoming packet from one of the internal and external networks, a black zone server coupled to the packet duplicating module for analyzing the duplicated packet, and an inspection engine coupled to the packet duplicating module and the [block] black zone server for inspecting whether the received incoming packet corresponds to the selected packet to be blocked based on the analysis in the [block] black zone server, wherein the black zone server serves as at least one of an intrusion detection system, an anti-virus system and a noxious site blocking system.

The paragraph at page 6, line 26, is revised as follows:

Figs. 3A and 3B offer schematic diagrams of conventional and other Internet-based VPNs;

The paragraph at page 12, line 5, is revised as follows:

The first memory 30 is used to store the packet, an OS (operating system), OS parameters, pre-defined parameters, IP addresses, [and] etc. The first memory 30 includes several types of high speed memory devices such as a DIMMM type 64-512 Mybte SDRAM, a flash type 4-8 Mbyte ROM. The first memory 30 further stores instructions for controlling actions to take on the incoming and outgoing packets. These instructions include a predetermined set of criteria based upon the fields of the incoming and other information such as the time of day at which the incoming packet was sent or received, and the state of the session. Such criteria can be implemented by inspecting the fields of the incoming packets, by reference to external data such as a connection status and the time of day and by reference to pre-defined tables or other information stored in the first memory 30. The application of the criteria leads one or several pre-defined actions to be taken on the incoming packet.

The paragraph at page 12, line 23, is revised as follows:

The VPN processor 60 performs tunneling using the IPSec (Internet Protocol Security) protocol, data encryption/[ ]decryption and packet authentication. It should be appreciated that the VPN processor 60 and the firewall processor 10 can be implemented by a single micro-processor or by a multiplicity of micro-processors in the present invention.

APPENDIX B

In the Claims:

Please amend claim 1 as follows:

1. An integrated security gateway apparatus interfacing with an internal network and an external network for blocking a selected packet from the internal network or external network, comprising:

a packet duplicating module for receiving and duplicating an incoming packet from one of the internal and external networks;

a black zone server coupled to the packet duplicating module for analyzing the duplicated packet; and

an inspection engine coupled to the packet duplicating module and the [block] black zone server for inspecting whether the received incoming packet corresponds to said selected packet to be blocked based on the analysis in the [block] black zone server,

wherein said black zone server serves as at least one of an intrusion detection system, an anti-virus system and a noxious site blocking system.

APPENDIX C

In the Abstract:

Please amend the Abstract as follows.

A networking system of the present invention is associated with an integrated security gateway for integrating virtual private networking, firewall, and network monitoring functions. A duplicate of a received packet is provided to a network monitoring system connected thereto or included therein so as to detect all kinds of intrusions and attacks to a virtual private network and the integrated security gateway itself. And, by implementing a variety of functions and services in the network monitoring system, the network system of the present invention can enjoy almost complete security.